



La portabilité des données et des services

François Pellegrini

► To cite this version:

François Pellegrini. La portabilité des données et des services. *Revue française d'administration publique*, 2018, Les données publiques, 167 (3), pp.513-523. 10.3917/rfap.167.0513 . hal-01975442

HAL Id: hal-01975442

<https://inria.hal.science/hal-01975442>

Submitted on 9 Jan 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

La portabilité des données et des services

François Pellegrini

Université de Bordeaux, LaBRI & Inria Bordeaux - Sud-Ouest, 351 cours de la Libération, 33405 Talence cedex, France. francois.pellegrini@labri.fr

Résumé

La réduction de l'asymétrie entre usagers et responsables de traitements informatisés nécessite la création de droits adaptés. Tel est le cas du droit à la portabilité pour les services numériques. Ce droit est à la fois un droit économique, prolongeant le droit à l'interopérabilité, et un droit des personnes, participant à garantir leur autodétermination informationnelle. Ses deux sources en France sont, d'une part, le règlement général sur la protection des données, adopté au niveau européen, et, d'autre part, la loi pour une République numérique. La mise en œuvre pratique de ce droit, tant par les acteurs privés que publics, est de nature à réduire les effets de rente et favoriser la création de services nouveaux.

La révolution numérique dans laquelle l'humanité est actuellement plongée peut déjà être décomposée en quatre phases. À l'âge de l'ordinateur (1950-1970), caractérisé par l'arrivée sur le marché des premiers ordinateurs commerciaux, a succédé l'âge du logiciel (1970-1990), bien immatériel au marché distinct de celui des ordinateurs. Vint ensuite l'âge des réseaux (1990-2010), au cours duquel le déploiement et la démocratisation des réseaux numériques ont conduit à l'interconnexion forte des personnes et des organisations. Celle-ci a permis la création de biens communs numériques (logiciels libres, Wikipedia, etc.) mais aussi des grands silos de données, majoritairement privés (les « GAFA » et autres « BATX », tels que Google, Apple, Facebook, Baidu, Alibaba, etc.). L'âge actuel (2010-...) est celui de la donnée. Il est caractérisé par la valorisation propre de la donnée par les grands silos, tant privés que publics. Ceux-ci disposent de capacités de stockage et de calcul considérables et peuvent ainsi mettre en œuvre des traitements à forte valeur ajoutée, tels que la recherche de corrélations au moyen d'outils de traitement de « mégadonnées », renforçant leurs positions dominantes.

La réduction de cette asymétrie nécessite de munir les personnes de droits adaptés à cette situation inédite. La pierre angulaire de ce nouvel édifice est le droit des données personnelles, qui se présente vis-à-vis des personnes concernées en tant que droit à l'« autodétermination informationnelle ». Ce droit, qui garantit « la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel », est considéré comme un droit de rang constitutionnel en Allemagne¹. Or, les personnes ne peuvent exercer en pratique leur autodétermination informationnelle que si elles disposent de la capacité effective de choisir l'acteur à qui elles confient le traitement de leurs données. Il est donc nécessaire que la loi leur donne les moyens de quitter un responsable de traitement indélicat ou inefficace avec lequel elles sont déjà en relation, au profit d'un de ses concurrents. Afin de stimuler l'innovation, les personnes doivent également pouvoir expérimenter un nouveau service, en parallèle de ceux qu'elles utilisent déjà, en lui apportant les données qu'elles ont déjà confié à ces services préexistants. Tel est le rôle du « droit à la portabilité » qui se construit actuellement.

Le droit à la portabilité s'inscrit dans la vision personnaliste du droit des données personnelles. Ces dernières, à l'instar de tout bien non rival, ne peuvent rationnellement relever d'un régime de propriété (I). Il garantit de façon effective la réutilisation de certaines catégories de données, là où des droits plus anciens, conçus dans le but de favoriser globalement la récupération des données numériques à fin de réutilisation, étaient mis à mal par l'évolution des technologies (II). Il se construit au travers de sources multiples (III), qui définissent des modalités de mise en œuvre différentes selon les catégories de données (IV). Des dispositions spécifiques visent à aider les personnes dans la mise en œuvre effective de la portabilité de leurs données, contribuant à l'émergence d'une portabilité des services (V). Pour autant, l'intégralité des données détenues par les responsables de traitement sur les personnes n'a pas vocation à être communiquée à fin de réutilisation (VI).

I.— Statut de la donnée

Une lecture superficielle de la législation pourrait laisser croire qu'il n'existe pas de régime juridique uniforme de la donnée. En effet, seules certaines catégories de données font l'objet de dispositions *ad hoc* au sein de textes

1. Le droit à l'autodétermination informationnelle (« *Informationnelle Selbstbestimmung* ») a été proclamé pour la première fois par la Cour constitutionnelle fédérale de l'Allemagne, dans un arrêt du 15 décembre 1983. Il est pour elle une conséquence des articles 1^{er} (dignité de l'homme) et 2 (droit au libre développement de sa personnalité) de la Loi fondamentale (« *Grundgesetz* »), dont la Cour déduit que : « la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel » (Conseil d'État, 2014, 267).

législatifs distincts : droit d’auteur régulant les œuvres de l’esprit, droit des données à caractère personnel², droit des producteurs de bases de données³, etc.⁴ Cette absence définit néanmoins, en creux, un régime juridique uniforme : celui de la libre réutilisation des biens immatériels. Cette liberté générale de copie et de réutilisation de la donnée n’est bridée que dans les cas où la totale liberté serait susceptible de porter atteinte à d’autres droits, les restrictions mises en place devant l’être dans l’intérêt général. Telle est par exemple la justification des droits patrimoniaux sur les œuvres de l’esprit, créés dans le but d’encourager globalement la création⁵, ou encore le droit au respect de la vie privée, pour les données relatives aux personnes.

La non-rivalité des données rend par essence inadéquat tout régime de propriété les concernant. C’est une vieille lune, régulièrement remise au goût du jour, que d’imaginer soumettre les données, et en particulier les données personnelles, à un régime de propriété, au prétexte de les « valoriser ». Pour se convaincre de l’absurdité de la chose, il suffit de prendre un exemple historique : celui de la masse critique de l’uranium. Cette donnée représente la masse d’uranium nécessaire au déclenchement d’une réaction de fission nucléaire en chaîne, et est donc un élément essentiel pour la construction de l’arme atomique. Au cours de la Seconde Guerre mondiale, les États-Unis ont investi des sommes considérables pour la déterminer, dans le cadre du projet Manhattan. En sont-ils pour autant les « propriétaires » ? Lorsque les Soviétiques, poursuivant des travaux similaires, sont eux aussi parvenus à déterminer cette donnée, ont-ils « volé » la « propriété » des États-Unis ? Un nouveau « copropriétaire » est-il apparu ? Pourtant, les Soviétiques ont pu décider de la fournir à leurs alliés sans demander la permission des États-Unis, ce qui n’aurait pu se faire si propriété il y avait eu. Cet exemple montre que le statut de la donnée ne peut se penser à l’aune de la propriété. Comment interdire à un tiers de collecter ou d’utiliser de façon indépendante une donnée, au prétexte qu’elle serait déjà « possédée », parfois de façon secrète ?

Il en est de même des données personnelles. En premier lieu, il serait incohérent de soumettre les données personnelles à un régime de propriété alors que les données en général ne le seraient pas, sachant que la frontière entre les deux est très ténue. Par exemple, la courbe de charge électrique, qui mesure la consommation électrique d’un abonné à intervalles de temps réguliers, n’est pas une donnée à caractère personnel lorsqu’elle concerne un site industriel. En revanche, lorsqu’elle concerne le domicile d’une personne, elle peut révéler le film qui est regardé si son pas d’échantillonnage est inférieur à deux secondes (Greveler *et al.*, 2012). Un autre exemple est celui du nom de famille d’une personne, ou son patrimoine génétique. Ils ne peuvent lui « appartenir », puisqu’ils sont partagés, au moins partiellement, tant par son ascendance que sa descendance et ses collatéraux, sans qu’elle puisse se prévaloir d’un quelconque statut de « copropriétaire ». Ici encore, la nature non rivale de ces biens empêche toute mise en œuvre d’un principe de propriété.

L’idée d’un régime de propriété sur les données personnelles est en fait promue par certains cercles économiques, qui cherchent à rallier à leur cause les personnes (co-)productrices de données en leur faisant miroiter les revenus qu’elles pourraient tirer de leur monétisation. Or, le montant unitaire qu’une personne pourrait recevoir n’est estimé au mieux qu’à quelques euros et, une fois la « propriété » des données transférée, ce transfert serait irrévocable. Cela conduirait les acteurs les plus riches à bénéficier de monopoles sur des stocks de données, freinant l’innovation en privant les nouveaux entrants innovants de l’accès à ces stocks de données, que les personnes ne pourraient plus confier à nouveau.

Le fait que les données ne relèvent pas d’un régime de propriété ne s’oppose pour autant pas à la régulation de leur usage. Ainsi les personnes, tant physiques que morales, productrices de données, se voient-elles confier des droits exclusifs sur celles-ci par différentes lois sectorielles. Ces personnes disposent ainsi d’un portefeuille⁶ de droits portant sur des biens informationnels, transmissibles ou non selon les catégories, et sur lequel elles peuvent concéder, sous condition, certains droits à des tiers. La maîtrise de son portefeuille informationnel peut ainsi se définir comme la liberté de gérer les données dont on est l’ayant droit⁷.

II.— Marchés captifs et interopérabilité

Dans le monde numérique, la gestion des données des personnes et des organisations est partiellement ou totalement déléguée à des intermédiaires techniques (fabricants d’ordinateurs et de réseaux, concepteurs de logiciels, responsables de traitements, etc.). Ces derniers peuvent, par leurs actions, et en particulier leurs choix de conception, brider la liberté d’action des ayants droit.

2. Que nous appellerons de façon abrégée « données personnelles », suivant en cela l’usage courant, qui ne doit pourtant pas faire oublier leur dénomination réelle.

3. Ce droit *sui generis*, spécifique à l’Union européenne, a été créé par la directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données. Il rattache artificiellement au droit d’auteur un droit économique qui relève, dans les autres régions du monde, de la concurrence déloyale.

4. L’ensemble des droits sur les biens immatériels est parfois désigné sous l’appellation « fourre-tout » de « propriété intellectuelle ». Ce terme est inadéquat, dans la mesure où il présuppose que ces droits auraient des caractéristiques similaires à celle de la propriété sur les biens matériels. Ce n’est absolument pas le cas, comme il sera démontré plus loin.

5. Le moyen choisi pour cela étant de créer une restriction temporaire d’accès au domaine public, le régime général de libre circulation des œuvres qu’elles rejoindront une fois ces droits échus.

6. Le terme de « patrimoine » pourrait ici encore prêter à confusion, du fait de sa connotation « propriétaire ».

7. Ce terme doit ici être pris au sens large, et non dans la seule acception du droit d’auteur qui n’est, comme on l’a vu, qu’un régime parmi d’autres de régulation de l’usage d’une catégorie de données.

L'un des principaux moyens mis en œuvre par ces intermédiaires pour contrôler leurs clients et/ou usagers consiste à capturer leurs données au sein d'écosystèmes opaques. C'est le cas par exemple lorsque les données sont encodées au sein de formats de données fermés. La personne qui a confié ses⁸ données peut alors se voir refuser le libre accès ultérieur à celles-ci, si elle ne satisfait pas aux conditions imposées par le prestataire : renouvellement d'abonnement, achat de licence de la nouvelle version du logiciel adéquat, etc. C'est pour lutter contre ces rentes indues que le législateur européen a introduit, au sein de la directive 91/250/CE⁹, des dispositions destinées à lutter spécifiquement contre elles : il s'agit de celles relatives la décompilation à fin d'interopérabilité.

Le droit d'auteur adapté au logiciel¹⁰ a été conçu par le législateur européen de façon à garantir les conditions d'une concurrence libre et non faussée au sein de ce secteur. Pour cela, il consacre le fait de pouvoir s'inspirer des fonctionnalités d'un logiciel existant afin de réaliser un logiciel équivalent, par l'observation externe, en « boîte noire », de ses fonctionnalités¹¹, tout en interdisant la concurrence déloyale consistant à analyser ou à reprendre tout ou partie du code existant. Le but de ces dispositions est que le concurrent potentiel supporte sensiblement les mêmes délais et coûts de développement que l'auteur du logiciel initial, afin que ce dernier ait le temps de se rembourser de ses investissements et d'améliorer son logiciel initial, stimulant ainsi l'innovation et la concurrence.

La seule exception à ces dispositions est motivée par la nécessité de permettre à un concurrent de comprendre la façon dont un logiciel encode ses données, afin de réaliser un logiciel interopérable avec l'existant¹². Pour cette seule finalité, elle autorise l'étude de la partie correspondante du code du logiciel initial, voire la recopie pure et simple de cette partie. Ces dispositions visent à briser les monopoles de rente sur les données captives, en permettant à quiconque de comprendre comment les données ont été encodées, et de les extraire de leur écosystème logiciel fermé.

Cependant, ces dispositions protectrices, pensées à l'âge du logiciel, ne sont plus opérantes aujourd'hui. En premier lieu, la généralisation de l'informatique en nuage (« *cloud computing* ») fait qu'il n'est plus possible aux usagers d'avoir accès, à fin d'étude, au code du logiciel traitant leurs données, celui-ci étant situé sur des serveurs distants et inaccessibles. En deuxième lieu, même s'il était possible d'en extraire l'information nécessaire, ces dispositions ne permettent pas d'imposer au responsable de traitement de mettre en œuvre un accès aux données permettant l'exécution d'un logiciel d'extraction et de transcodage. En troisième lieu, le coût économique de la rétro-ingénierie constitue encore une barrière à l'entrée importante pour les nouveaux acteurs, d'autant que la généralisation des outils numériques a fait exploser le nombre de traitements concernés.

Le droit à la portabilité remédie à l'ensemble de ces contraintes. Là où le droit à l'interopérabilité régule les rapports entre producteurs de logiciels, au bénéfice indirect de leurs usagers, le droit à la portabilité concerne directement les usagers. Il conduit à reporter sur le responsable de traitement l'obligation de mettre en œuvre les moyens techniques permettant aux usagers d'un système d'en extraire à fin de réutilisation les données qu'ils y ont introduites. Il réduit le coût économique de l'interopérabilité, en le faisant essentiellement supporter par l'acteur disposant par nature et sans frais additionnels de l'information la plus complète sur l'encodage des données : le concepteur du logiciel.

III.— Deux sources pour un même droit

Le droit à la portabilité est à la fois un droit économique, prolongeant le droit à l'interopérabilité, et un droit des personnes, participant à garantir leur autodétermination informationnelle. Cette dualité transparaît clairement au travers des textes qui le définissent.

En tant que droit des personnes, il est défini, au niveau européen, par l'article 20 du Règlement général sur la protection des données¹³ (RGPD). Ce texte dispose que : « Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement [...] et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque : a) le traitement est fondé sur le consentement [...] ou sur un contrat [...]; et b) le traitement est effectué à l'aide de procédés automatisés. [...] ».

En tant que droit économique, il a été prévu, au niveau national, par l'article 48 de la loi pour une République numérique¹⁴ (LRN), visant à créer les articles L. 224-42-1 et suivants du code de la consommation. Cet article dispose

8. Nous désignerons par le possessif le fait que la personne soit l'ayant droit desdites données, et non qu'elle en soit la « propriétaire », voir *supra*.

9. Directive du Conseil du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur (91/250/CE), Journal officiel n° L. 122 du 17/05/1991, pp. 0042-0046.

10. Les logiciels disposent, dans le Code de la « propriété intellectuelle », d'amodiations qui les soumettent quasiment à un droit *sui generis* (Pellegrini et Canevet, 2013, 97).

11. Article 5.3 de la directive 91/250/CE, transposé en l'article 122-6-1 III du CPI : « La personne ayant le droit d'utiliser le logiciel peut sans l'autorisation de l'auteur observer, étudier ou tester le fonctionnement ou la sécurité de ce logiciel afin de déterminer les idées et principes qui sont à la base de n'importe quel élément du logiciel lorsqu'elle effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du logiciel qu'elle est en droit d'effectuer. » Ces dispositions ne font que rappeler l'évidence, à savoir que les idées sont de libre parcours.

12. Article 6 de la directive 91/250/CE, transposé en l'article 122-6-1 IV du CPI : « La reproduction du code du logiciel ou la traduction de la forme de ce code n'est pas soumise à l'autorisation de l'auteur lorsque la reproduction ou la traduction [...] est indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels [...] ».

13. Règlement du Parlement européen et du Conseil n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

14. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

que : « Le consommateur dispose en toutes circonstances d'un droit de récupération de l'ensemble de ses données. Cette récupération s'exerce conformément aux conditions prévues à l'article 20 du [RGPD] pour les données ayant un caractère personnel, et à la présente sous-section pour les autres. [...] tout fournisseur d'un service de communication au public en ligne propose au consommateur une fonctionnalité gratuite permettant la récupération : 1° De tous les fichiers mis en ligne par le consommateur ; 2° De toutes les données résultant de l'utilisation du compte d'utilisateur du consommateur et consultables en ligne par celui-ci, à l'exception de celles ayant fait l'objet d'un enrichissement significatif par le fournisseur en cause [...] 3° D'autres données associées au compte utilisateur du consommateur [...] ».

Le « Groupe de travail de l'article 29 sur la protection des données » (G29), dans les lignes directrices qu'il a publiées sur la portabilité des données (G29, 2017), précise l'interprétation que les autorités de protection des données de l'Union européenne entendent donner à la notion de données « fournies à un responsable de traitement ». Il s'agit tant des données explicitement fournies par les personnes, que des données induites par l'usage du service (par exemple, la courbe de charge de la consommation électrique) ou des informations de contexte (« métadonnées ») que le responsable de traitement a pu collecter dans le cadre de l'interaction avec l'utilisateur (informations d'horodatage, etc.). Pour autant, le responsable de traitement n'a aucunement l'obligation de collecter, ni de conserver outre mesure, des catégories de données qui pourraient éventuellement être utiles à l'utilisateur mais non nécessaires au traitement. La portabilité des données n'a ainsi aucunement vocation à s'opposer au principe protecteur de minimisation des données collectées et conservées.

Le droit national, pour sa part, vise à étendre le droit à la portabilité à des catégories de données qui ne sont pas nécessairement à caractère personnel, puisqu'elles concernent l'intégralité des contenus fournis par l'utilisateur au service et conservés par celui-ci. Par exemple, dans le cadre d'un réseau social, cela concerne l'intégralité des contenus déposés et stockés sur celui-ci : messages, images, vidéos, bases de données, etc.

IV.— Modalités fonctionnelles et techniques

Les modalités de mise en œuvre de la portabilité des données s'inscrivent pleinement dans le cadre de la numérisation de la société, puisqu'elles font explicitement référence à des considérations informatiques. Ainsi l'article 20 du RGPD dispose-t-il que les données personnelles transmises doivent l'être « dans un format structuré, couramment utilisé et lisible par machine », alors que le 2° de l'article L. 224-42-3 à venir du code de la consommation dispose pour sa part que : « toutes les données résultant de l'utilisation du compte d'utilisateur du consommateur et consultables en ligne par celui-ci [...] sont récupérées dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé ».

À ce titre, la LRN est plus ambitieuse que le RGPD. Ce dernier n'exige en effet qu'une simple compatibilité¹⁵ entre systèmes, les données restituées devant être encodées dans « un format structuré, couramment utilisé », ce qui permet de considérer comme satisfaisants des formats de données fermés dès le moment où ils correspondent à des standards du marché. La LRN, en revanche, met en œuvre les principes de l'interopérabilité, à travers ses principaux attributs : l'utilisation d'un standard ouvert et la loyauté du responsable de traitement vis-à-vis de la facilité de réutilisation des données encodées dans le format en question. L'exigence d'ouverture est une obligation de moyens pesant sur le responsable de traitement. Ainsi, l'article L. 224-42-3 dispose-t-il également que : « Lorsque les données collectées auprès du consommateur ne peuvent pas être récupérées dans un standard ouvert et aisément réutilisable, le fournisseur de service de communication au public en ligne en informe le consommateur de façon claire et transparente. Le cas échéant, il l'informe des modalités alternatives de récupération de ces données et précise les caractéristiques techniques du format du fichier de récupération, notamment son caractère ouvert et interopérable. » Il ressort de ces dispositions que les usagers seront en droit de demander au responsable de traitement les raisons pour lesquelles il n'est pas en mesure de fournir les données sous un format ouvert.

La LRN va encore plus loin, puisqu'elle organise les modalités pratiques de restitution des données par le responsable de traitement. L'article L. 224-42-3 dispose ainsi également que : « La fonctionnalité prévue au premier alinéa permet au consommateur de récupérer, par une requête unique, l'ensemble des fichiers ou données concernés. Le fournisseur prend toutes les mesures nécessaires à cette fin, en termes d'interface de programmation [...] ».

Les rédacteurs du RGPD, soucieux de rester dans le cadre du droit des personnes et de ne pas empiéter ouvertement dans le domaine de la régulation économique, marchent sur un chemin étroit. Ainsi, dans le même considérant 68, est-il énoncé, d'une part, qu'« [i]l y a lieu d'encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données » mais que, d'autre part, « [l]e droit de la personne concernée de transmettre ou de recevoir des données à caractère personnel la concernant ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles ». Ces deux positions sont antagonistes par nature : la pression du public pour disposer d'un service de portabilité le plus efficace possible ne peut que conduire les différents acteurs à accepter les jeux de données les plus riches possibles de la part de leurs concurrents, et donc à une convergence fonctionnelle sur des enjeux d'interopérabilité tels que l'identification des personnes et des entités auxquelles elles sont liées : établissements scolaires, entreprises, associations, etc. (voir *infra*).

15. Pour une discussion approfondie des différences entre compatibilité et interopérabilité, voir (Pellegrini et Canevet, 2013, 255).

V.— La portabilité des données dans le secteur public

En tout état de cause, les responsables de traitements publics situés en dehors de la sphère commerciale ne sont pas concernés par les dispositions de la LRN, mais seulement par celles du RGPD pour les données à caractère personnel. Or, celui-ci leur permet de s'en exonérer, puisque le 3° de l'article 20 du RGPD dispose précisément que le droit à la portabilité des données « ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ». Si l'on peut avancer, comme justification à cette dérogation, l'argument fonctionnel que l'administration ne peut par nature avoir de concurrente à qui les données pourraient être transmises, les considérations économiques n'en sont sûrement pas absentes non plus : le coût de mise en conformité des divers systèmes d'information de l'État et des collectivités, dont certains datent d'avant l'âge des réseaux, peut être considéré à bon droit comme insupportable.

Pour autant, les acteurs publics ont tout intérêt à intégrer à leurs nouveaux téléservices les moyens permettant aux usagers d'obtenir, sous une forme facilement exploitable par une machine, l'ensemble des données que ceux-ci ont fournies (G29, 2017, note 36). Cette pratique pourrait utilement concerner tous types de données, y compris celles n'étant pas à caractère personnel, telles que les données relatives aux entreprises. La restitution, sous un format ouvert et homogène, de données qui ont pu être élaborées au cours du temps, sur des logiciels différents et non nécessairement interopérables, par les acteurs économiques les moins outillés (TPE, PME), constitue un service à valeur ajoutée qui ne peut que bénéficier à ceux-ci. Elle faciliterait leur migration vers les systèmes compatibles avec le format mis en œuvre par la puissance publique, et inciterait à la fourniture de services complémentaires innovants utilisant ces données et basés sur ces mêmes formats.

VI.— La portabilité, des données aux services

Le principe de portabilité peut être envisagé à deux niveaux. Le premier, le plus basique, consiste en la capacité pour la personne à obtenir copie des données qu'elle avait confiées au responsable de traitement. Il s'agit là d'une version étendue du droit d'accès, en renforçant les obligations des responsables de traitement en ce qui concerne le formatage, à fin de traitement ultérieur, des données devant être restituées aux usagers. De telles modalités ont déjà été envisagées par le passé pour certaines catégories de données, telles que les données de santé. Plusieurs pays ont ainsi lancé des initiatives et modifié leur législation dans le but de favoriser le partage des données personnelles de santé entre les acteurs de la santé et leurs patients. Tel est le cas de l'initiative « *Blue Button* » (Chopra, 2010) aux États-Unis et, en France, du « Dossier médical partagé »^{16 17}. Ces initiatives s'inscrivent dans une dynamique globale tendant à rendre les personnes actrices de la gestion de leurs données. Alors que cette gestion était autrefois essentiellement placée entre les mains de professionnels, les individus y prennent une part de plus en plus active, en particulier au sein d'associations de patients.

Pour autant, peu de personnes disposent des compétences leur permettant de manipuler elles-mêmes les masses de données qui leur sont transmises. C'est pour cela que la portabilité est également envisagée à un second niveau : celui des services. Il s'agit pour la personne de pouvoir faire transférer directement ses données d'un prestataire à l'un de ses homologues, sans avoir à les récupérer elle-même au préalable. Le 2° de l'article 20 du RGPD dispose ainsi que : « Lorsque la personne concernée exerce son droit à la portabilité des données [...], elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible ». L'article L. 224-42-3 envisagé par la LRN dispose pour sa part que : « Le fournisseur prend toutes les mesures nécessaires [...] en termes [...] de transmission des informations nécessaires au changement de fournisseur ».

Le but affiché de ces dispositions est de permettre à l'utilisateur un changement de prestataire le plus fluide possible, à l'image de ce qui a été mis en place dans le secteur de la téléphonie mobile. Pour autant, dans le monde des services numériques, chaque acteur se différencie souvent des autres par un positionnement et des services distincts de ses concurrents. Une portabilité permettant aux personnes de retrouver à l'identique l'ensemble des services est donc difficilement envisageable, d'autant que le fait de retrouver de telles fonctionnalités suppose de transmettre des données qui ne concernent pas directement les personnes, voire concernent d'autres personnes. Par exemple, pour qu'une personne souhaitant faire migrer ses données d'un réseau social à un autre retrouve la connectivité de ses connaissances, il faudrait pouvoir exporter suffisamment d'informations identifiantes desdites connaissances pour les corréler aux informations disponibles sur le réseau social de destination et rétablir autant que possible les connectivités rompues. Un tel traitement ne peut se faire qu'avec le consentement de ces personnes, vraisemblablement acquis lors de l'acceptation des conditions générales d'utilisation du site de destination, mais aussi du site d'origine, afin d'autoriser l'exportation partielle d'informations identifiantes. Le RGPD anticipe ce cas de figure, en rappelant dans son considérant 68 que « [l]orsque, dans un ensemble de données à caractère personnel, plusieurs personnes sont concernées, le droit de recevoir les données à caractère personnel devrait s'entendre sans préjudice des droits et libertés des autres personnes concernées conformément au présent règlement ». L'article 20 en prend acte, en disposant dans son 4° que : « [c]e droit [...] ne porte pas atteinte aux droits et libertés de tiers ».

16. Ce projet à l'histoire complexe a été relancé par la loi n° 2016-41 « de modernisation de notre système de santé » du 26 janvier 2016.

17. En ce qui concerne les réflexions sur des analogues au « *Blue Button* », voir par exemple (Albarède et Molins, 2016).

Le coût de la portabilité à supporter par les responsables de traitement est donc à la fois un coût « de sortie », lié à la mise à disposition des modules et interfaces de programmation permettant l'exportation des données, mais aussi un coût « de rentrée », permettant l'importation de données issues d'un tiers au sein de son environnement. Le coût de sortie peut être problématique pour des systèmes anciens, dans lesquels la structuration des mécanismes de stockage n'a pas été pensée avec cette fonctionnalité en tête. Le coût de rentrée est pour sa part difficile à évaluer, car il dépend de la nature et de l'interdépendance des données considérées. Il doit être considéré comme un investissement, puisque la capacité à accueillir facilement de nouveaux usagers, y compris ceux provenant de plateformes offrant un service complémentaire, est un facteur déterminant de la croissance des écosystèmes de plateformes (Engels, 2016).

En tout état de cause, fournir aux usagers une portabilité de service efficace suppose une concertation entre les acteurs, vraisemblablement au sein de leurs associations professionnelles, afin de dégager des standards et procédures communs. Ce chantier s'annonce comme vaste. L'interopérabilité qui en émergera ne pourra que contribuer au peuplement rapide de nouveaux services innovants et à la fluidification accrue du marché. Ce besoin peut également susciter l'émergence d'intermédiaires dédiés, agissant pour le compte des personnes et offrant des services de portabilité étendus, par exemple en recréant les connectivités perdues au moyen de gisements de données tiers qu'ils alimenteront par leur pratique.

VII.— Restrictions à la portabilité

Le nouveau droit à la portabilité n'est pas absolu, au sens qu'il ne concerne pas l'intégralité des données relatives aux personnes concernées. En effet, le législateur a considéré le cas dans lequel les données brutes fournies par les personnes auraient fait l'objet d'un traitement subséquent dit « d'enrichissement », au cours duquel elles ont pu être corrélées à d'autres sources de données (données démographiques, économiques, etc., mais aussi données personnelles des autres usagers) afin de produire des connaissances nouvelles. Dans un tel cas, les données enrichies ne contiennent pas la seule valeur apportée par l'utilisateur, mais un agrégat issu de sources multiples, qu'il pourrait être considéré comme anti-concurrentiel de transmettre à fin de réutilisation par un concurrent.

C'est pour ces raisons que tant le RGPD que la LRN mettent en place des dispositions limitatives. Pour le RGPD, le 1^{er} de l'article 20 restreint la restitution aux seules « données à caractère personnel les concernant qu'elles ont fournies » (ainsi que les métadonnées résultant de l'interaction de la personne avec le service, voir *supra*), excluant *a contrario* toute donnée ayant fait l'objet d'un enrichissement. La LRN est, ici encore, plus ambitieuse. L'article L. 224-42-3 envisagé par elle dispose en son 2^o que doivent être fournies par le responsable de traitement « toutes les données résultant de l'utilisation du compte d'utilisateur du consommateur et consultables en ligne par celui-ci, à l'exception de celles ayant fait l'objet d'un enrichissement significatif par le fournisseur en cause ». Tout comme pour le RGPD, l'idée du législateur est de pouvoir restituer à l'utilisateur des informations de contexte et métadonnées issues du traitement de ses données par le responsable de traitement (comme par exemple l'horodatage des messages postés sur le « mur » d'un réseau social), tant que cette fourniture ne lui cause pas un préjudice injustifié.

Il s'agira donc pour les responsables de traitement de justifier du caractère « significatif » de l'enrichissement, et en quoi la fourniture de données enrichies leur serait préjudiciable. On peut penser aux catégories de profilage mises en œuvre par certaines régies publicitaires, qu'elles ne souhaitent pas voir divulguer, de façon indirecte, à leurs concurrents. Il s'agira donc pour les responsables de pouvoir éventuellement produire, à fin d'exportation, des données « des-enrichies », sans pour autant qu'elles soient plus pauvres que les données brutes initialement fournies, ni que cet appauvrissement nuise à la portabilité effective du service en question.

Conclusion

La généralisation des traitements de données offerts aux personnes rend plus visible et insoutenable la création de rentes et de marchés captifs construits autour des données traitées. La prise de conscience des effets pervers de ces rentes conduit à la construction de droits nouveaux, visant à rééquilibrer les rapports entre les responsables de traitements et leurs usagers.

Dans ce contexte, la création du droit à la portabilité est une initiative originale et bienvenue. Ce droit est cependant encore incomplet, car il ne concerne à l'heure actuelle que deux catégories de données : les données personnelles (qui constituent cependant un gisement essentiel de données captives) et les données liées à l'utilisation des services numériques par les particuliers, pris sous l'angle du droit des consommateurs. Or, il semble qu'on se trouve là en face d'un droit plus général, concernant tant les personnes physiques que morales, destiné à prolonger à l'ère de la donnée le droit à l'interopérabilité ébauché à l'ère du logiciel.

Ce droit pourrait sans dommage s'étendre à tous les systèmes informatiques, et non aux seuls services de communication au public en ligne. Plus largement, des dispositions équivalentes pourraient être prises afin d'offrir ces possibilités à tout usager d'un système numérique, y compris dans un cadre professionnel (CNNum, 2017). Ce droit à la portabilité généralisé apparaîtrait ainsi tel qu'il est : un analogue numérique du droit à la liberté d'association, permettant la libre interaction entre services et leurs usagers à l'ère numérique. Il s'agirait de ce fait d'un droit de rang constitutionnel, comme l'illustre déjà, dans le cas des données à caractère personnel, son rattachement au droit à l'autodétermination informationnelle, pour sa part déjà en cours de constitutionnalisation.

Références

- Albarède, Marine et Molins, Manon (2016), « MesInfos Santé – Vers un *Blue Button* à la française », FING, http://mesinfos.fing.org/wp-content/uploads/2016/05/MesInfos_Sante_Pages.pdf.
- Chopra, Aneesh (2010), « *'Blue Button' Provides Access to Downloadable Personal Health Data* », blog de la Maison Blanche, 7 octobre 2010, <https://www.whitehouse.gov/blog/2010/10/07/blue-button-provides-access-downloadable-personal-health-data>.
- Conseil d'État (2014), *Le numérique et les droits fondamentaux*, Étude annuelle, Paris, La Documentation française, <http://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-etat-le-numerique-et-les-droits-fondamentaux>.
- Conseil national du numérique (CNNum) (2017), « Avis sur la libre circulation des données dans l'Union européenne », avril 2017, https://cnnumerique.fr/files/2017-10/AvisCNNum_FFoD_VFinale.pdf.
- Engels, Barbara (2016), « Data portability among online platforms », Internet Policy Review, 5(2), DOI : 10.14763/2016.2.408, <https://policyreview.info/articles/analysis/data-portability-among-online-platforms>.
- G29 (« Groupe de travail de l'article 29 sur la protection des données ») (2017), « Lignes directrices relatives au droit à la portabilité des données », 16/FR WP 242 rev. 01, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48.
- Greveler, Ulrich; Justus, Benjamin; Loehr, Dennis (2012), « *Multimedia content identification through smart meter power usage profiles* », Computers, Privacy and Data Protection (CPDP).
- Pellegrini, François et Canevet, Sébastien (2013), *Droit des logiciels*, Puf.